

eLab Forensics LLC

Cellebrite Reports - 2021 Quick Start User Guide

Pratical Solutions to digital Evidence for Public Defenders



Quick start user guide for opening, navigating and creating custom reports in Cellebrite.



eLab Forensics LLC

P.O. Box 340355 Hartford, CT 06134

Phone: 877-266-3703 www.elabforensics.com infor@elabforensics.com

QUICK START USER GUIDE FOR CELLEBRITE EXTRACTION REPORTS

"For the legal team, by the legal team"

This guide is intended to assist the legal team in managing forensic reports obtained from a cell phone extraction created using Cellebrite.

The purpose of the guide is to create a basic, universal understanding of how to work with these reports. This includes the different levels of extractions, time zone settings, the components that make up an extraction report, the different types extraction report formats, and how to open, view and navigate these reports. In addition, this guide will show you how to search for specific data, create custom reports using the Cellebrite UFED Reader application and what to ask for when requesting reports.

CONTENTS

| ntroduction | .3 |
|---|----|
| evels of Extraction & Time Zone Settings | .3 |
| Report Components | .4 |
| 'DF Report | .5 |
| ITML Report | .7 |
| JFDR Report | .8 |
| JFDR Report – Search, Filter, Tag and Bookmark1 | 1 |
| Creating Custom Reports1 | .6 |
| Requesting Reports1 | 18 |
| Summary & Hints | 19 |

© 2020 eLab Forensics LLC

All rights reserved. This book or any portion thereof may not be reproduced or used in any manner whatsoever without the express written permission of the publisher except for the use of brief quotations in a book review.

INTRODUCTION

It is important to know what type of report was provided, what exactly is included and determining what time zone settings was used. This guide will explain the different report formats and how to use them, how different extraction levels can produce more or less results and how to verify the correct time settings.

EXTRACTION LEVELS

Depending on the device, there may be more than one method to extract data and it is not uncommon for more than one extraction to be conducted for the same device. It is important to know the difference between the different extraction levels because each one can recover a different amount of data. However, not all devices are supported for all extraction levels.



A logical extraction obtains the least amount of data. A file system extraction obtains the database files and may recover deleted data still present in the databases. A physical extraction will copy the entire device memory and will recover the most data. The type(s) of extraction conducted will be listed in the *Source Extraction* section of the Cellebrite Report.

TIME ZONES

On mobile devices, time stamp information for data items is stored in device memory in coordinated universal time (UTC) and is usually displayed to the device user in local time as obtained from the network. UTC is the primary time standard by which the world regulates clocks and time. UTC represents a vertical line drawn on the earth which crosses Greenwich, England. Time zones around the globe are applied either east or west of this line creating a negative (-) or positive (+) UTC offset. Daylight Saving Time (DST) can also attribute to this time offset based on the time of year.

On the east coast of the United States, Eastern Standard Time would be UTC -5:00 hours and during Daylight Saving Time would be UTC -4:00 hours. On the west coast, UTC -7:00 or UTC - 8:00 would be the correct negative (-) offset applied depending on the time of year and whether Daylight Savings Time is observed.

(For more information about setting time zones, see page 9)

REPORT COMPONENTS

A Cellebrite extraction report is usually provided on a disc or USB drive and will have several components which work together. The report will be in a folder that contains files and sub folders. It will <u>usually</u> be labeled by the type of device that was extracted, the device operating system version, type of extraction and the date and time of the extraction, but could vary.



Because of the size of these files it is recommended that the <u>entire folder</u> by copied to your desktop so opening and navigation will be faster.

Files & Sub-Folders

The folder may contain extraction reports in more than one format along with associated file folders containing link files. The extraction reports and link file folders need to remain together. The links will not work if both components are not provided or if the file and folders are not together. The three (3) most common Cellebrite report format types are:

- 1. PDF report (Adobe document report file)
- 2. HTML report (Web browser)
- 3. UFDR report (Cellebrite UFED Reader)

Components

The following image shows the contents of the sample report folder with the three (3) different Sample types, PDF, HTML and UFDR and associated link file folders. The folder should also contain a UFED Reader program needed to open the UFDR file and a UFED Reader manual on how to use the program and create custom reports. *(See page 7 for more information about the UFED Reader)*

| | iPhone4GSM_7.0-7.0.2_Physical_13-11-13_08-50-47_2020-08-14_Report.ufdr | UFDR File |
|-----------|--|------------------------|
| Reports | 🔁 iPhone4GSM_7.0-7.0.2_Physical_13-11-13_08-50-47_2020-08-14_Report | Adobe Acrobat Document |
| Reader 🤫 | iPhone4GSM_7.0-7.0.2_Physical_13-11-13_08-50-47_2020-08-14_Report | HTML File |
| Manual | CellebriteReader | Application |
| | Cellebrite_Reader_v7.35_Jun_2020_Eng | Adobe Acrobat Document |
| | thumbnails | File folder |
| | resources | File folder |
| | Passwords | File folder |
| | party_photos | File folder |
| Link file | 📜 pages | File folder |
| | 📙 Maps | File folder |
| | 📙 icons | File folder |
| | 📙 gps | File folder |
| | 📜 files | File folder |
| | 📙 email | File folder |
| | Chats | File folder |
| | | |

PDF REPORT

A Cellebrite PDF format report can contain links to associated multimedia files such as images, video and audio recordings. The report may display small thumbnail images for photos and videos. Clicking on the hyperlinks will open full-size images or files such as videos or voicemail recordings will be played by the associated program. The actual data is contained in the associated link file folders found on the same file level with the report. These components work together and must be kept in the same folder to work correctly.

| iPhone4GSM_7.0-7.0.2_Physical_13-11-13_08-50-47_2020-08-14_Report | Adobe Acrobat Document |
|---|------------------------|
| thumbnails | File folder |
| resources | File folder |
| Passwords | File folder |
| party_photos | File folder |
| 🦲 pages | File folder |
| Maps | File folder |
| icons | File folder |
| 📕 gps | File folder |
| 📙 files | File folder |
| 📕 email | File folder |
| chats | File folder |

Open Using Adobe Reader

The PDF report should be opened using Adobe Reader for the hyperlinks to function properly. Other Adobe programs such as Adobe Acrobat may result in errors when attempting to open the link files. To open the report with Adobe Reader, right click on the PDF report and select: *Open with > Adobe Reader*.



Navigating PDF Reports

When the PDF report is opened it will display a folder hierarchy structure or index in the left pane and the details will be displayed in the larger pane.

The details about the device extraction, date, type and examiner are in the Summary section located on the first few pages of the PDF report.

The UTC settings are displayed in the summary section.

Quick Navigation: Click on the folder in the index to jump to the desired report section.

| olders Index | Details | Time Zone Settings | | |
|------------------------------|--------------------------------------|-----------------------------------|---------------------------------|--|
| L | | | | |
| Bookmarks (4)) | Summary | | | |
| | Cellebrite Physical Analyzer version | 7.34.0.38 | | |
| E Summany | Report creation time | 8/14/2020 2:04:43 PM =04:00 | | |
| Source Extraction | Time zone settings (UTC) | (UTC-08:00) Los Angeles (America) | | |
| Device Information | Examiner name | INO | | |
| Image Hash Details | Location | at ab Personaias III C | | |
| Plugins | Casa nama | eLao Forensics LLC | | |
| Contents | Case name | Sample | | |
| Aggregated Application Usage | | | | |
| Call Log | | | | |
| Cell Towers | Source Extraction | | | |
| Chats | Physical | | | |
| 🖻 🖫 iMessage: +16155079714 | Connection type | Cable No. 110 | | |
| Native | Extraction | Cable No. 110 | | |
| IPhoneRecentsLog | Extraction type | Physical | Physical Network (1994) | |
| □ Native | Extraction (OFD) me data miegri | Not available | | |
| 🖻 🕼 SMS Spotlight Search | • • | | | |
| Native | | | | |
| B Snapchat | Device Information | | | |
| Native | | | | |
| Contacts | Name | Value | Source | |
| Cookies | Physical | | | |
| Device Events | Serial number | 7W043M88A4S | Taken from UFD extraction file: | |
| Emails | ECID | 000002CB8102F5F7 | Taken from UFD extraction file: | |
| Installed Applications | Board | n90ap | Taken from UFD extraction file: | |
| Instant Messages | iBoot (firmware) version | iBoot-1940.1.75 | Taken from UFD extraction file: | |
| GPS | CPID | 8930 | Taken from UFD extraction file: | |
| Locations | Capacity | 14GB | Taken from UFD extraction file: | |
| Log Entries | Passcode | cbrox | Taken from UFD extraction file: | |
| Maps | Extraction partition | User and System data | Taken from UFD extraction file: | |
| Mobile Cards | Apple ID | owenucash2@gmail.com | Accounts3.sqlite: 0x14E66 | |
| Passwords | iCloud account present | False | | |
| P Searched Items | Owner Name | iPhone | data ark plist: 0x430 | |
| | Owner Ivallie | 11 110110 | data data parte de to d | |
| SMC Mercaner | Model number | N90AP | preferences.plist: 0x8D | |

Keyword Searches

On the PDF report, searches can be conducted by using the *Ctrl+f* function and entering search terms in the dialog box.



HTML REPORT

An HTML (Hypertext Markup Language) style report is made up of a single document broken up into different sections with an index that will open the results in new tabs, displaying like a web page in a web browser. Firefox, Chrome or Microsoft Edge browsers are recommended since Internet Explorer (IE) is no longer supported. If IE is the default viewer, the HTML report can be opened using Chrome or Firefox using the "Open with" procedure described on page 4.

The basic information as to the device information and the extraction details are at the beginning of the report.

The contents section will be at the bottom and will contain an index of links along the left side that can be clicked on to open content areas in different tabs.

| Contents | | | | | |
|--|--------------------|--------------|-------|--------------|--|
| Туре | Included in report | | Total | | |
| Application Usage | 8 | | 8 | | |
| 🖕 Call Log | 13 | | 13 | | |
| 👻 Cell Towers | 45 | | 45 | | |
| Q Chats | 25 | (3 Deleted) | 25 | (3 Deleted) | |
| • iMessage: +16155079714 | 3 | (2 Deleted) | 3 | (2 Deleted) | |
| iPhoneRecentsLog | 1 | | 1 | | |
| SMS Spotlight Search | 16 | (1 Deleted) | 16 | (1 Deleted) | |
| Snapchat | 5 | | 5 | | |
| Ontacts | 9 | | 9 | | |
| 🕙 Cookies | 79 | (19 Deleted) | 79 | (19 Deleted) | |
| 🖂 Emails | 111 | (31 Deleted) | 111 | (31 Deleted) | |
| Installed Applications | 55 | | 55 | | |
| 🔛 Instant Messages | 1 | | 1 | | |
| 💷 Locations | 318 | (45 Deleted) | 318 | (45 Deleted) | |
| → Log Entries | 31 | | 31 | | |
| 🛄 Maps | 1 | | 1 | | |
| 🗋 Mobile Cards | 1 | | 1 | | |
| - Passwords | 27 | | 27 | | |
| O Powering Events | 38 | | 38 | | |
| SMS Messages | 35 | (4 Deleted) | 35 | (4 Deleted) | |
| A User Accounts | 7 | (1 Deleted) | 7 | (1 Deleted) | |
| User Dictionary | 44 | | 44 | | |

Searching

Use the *Ctrl+f* function to run keyword searches, but it will only work on the individual page tabs rather than from the main page.

*Note: Opening Link Files

While reviewing reports in HTML format it is important to know that clicking a web site link would automatically open the file from the internet which could contain adult content.

7

UFDR REPORT

The Cellebrite UFED Reader (UFDR) report is Cellebrite file that allows the user to conduct advanced searches, filtering, timeline queries, tags, bookmarks, and project savings as well as generate customized reports in multiple formats. It requires the Cellebrite UFED Reader program to open that should be included with the extraction. UFDR report allows the most flexibility and will resemble the Cellebrite dashboard the forensic examiner sees during the examination. It has an easy to navigate index along the left side column under analyze data and a quick navigation area under *Content*, all on the main screen. A Cellebrite UFED Reader user manual should also be included.

| | File | View Tools Report He | lp | | | Sea | rch Q | Advanced | [0] | ۰ |
|-------------------|--------------------|--|---|---|------------------|-------------------------|--------------------|----------|------------|-----|
| යි. Home | O iPh | م ف one4GSM_7.0-7.0.2_Phys | Welcome × • Extraction | Summary (1) × | | | | | | * × |
| C | Search | zed Data | Extraction Summary | | + Add extraction | Add external file | O Project settings | E Genera | te report | |
| Analyzed Data | › :: ، ر | Application (59) | ⊙ Extractions: 1 | n | | | | | | |
| E File Systems | > 🔒 > (1) | Contacts (22) Devices & Networks (93) (81) | Physical Extraction | n start date/time | | | | | | |
| ·Ö- Insights | > • | Location Related (282) (33) Media (15388) (32) | Extraction | end date/time home\Shared\eLab CELLEBRITE | | | | | | |
| S Taos | > 📮 | Messages (180) (45) Search & Web (148) (17) | Case Information Examiner name JNO | | Lo | cation eLab Fore | nsics LLC | | | |
| Ē | > \$ | System & Logs (31) User Accounts & Details (43) (1) | Case name Sample Device Info | | | Content | | | | 0 |
| | Data | files | Advertising Id (IDFA) #1 9CC Board n90 Capacity 14G CPID 893 | D8C87-3236-4294-B0D4 ap B 0 | | E Aggregated Applicatio | . 4 🤨 Call Log | 13 | | Î |
| Cloud | | Applications (704) (2) | Apple ID owe iCloud account present False | nucash2@gmail.com e | | (m) Cell Towers | 17 (31) | 25 (2) | | |
| | | Archives (12) (4) | Last Factory Restore Upgrade 9/27 Model number N90 | //2013 2:06:04 PM(UTC+0) (AP | | V Cell lowers | | 23 (8) | | |
| | | Databases (155) | OS Version iPho Owner Name iPho | ne OS 7.0.2 (11A501) ine | | Contacts | 22 🦸 Cookies | 79 (17) | | |
| | 8 | Documents (15) | ECID 000 Extraction partition Use | J02CB8102F5F7 r and Svstem data | ~ | | | | | ~ |
| | т | Text (612) (2) | | | | | | | | |

Open Using Cellebrite Reader

Click on CellebriteReader and the associated UFDR report should automatically open the home screen as displayed on page 7.

| |] iPhone4GSM_7.0-7.0.2_Physical_13-11-13_08-50-47_2020-08-14_Report.ufdr | UFDR File |
|---|--|------------------------|
| | Cellebrite_Reader_v7.35_Jun_2020_Eng | Adobe Acrobat Document |
| Œ | CellebriteReader | Application |
| | Passwords | File folder |
| | thumbnails | File folder |
| | icons | File folder |
| | gps | File folder |
| | pages | File folder |
| | party_photos | File folder |
| | resources | File folder |
| | Maps | File folder |
| | files | File folder |
| | email | File folder |
| | chats | File folder |
| | | |

8

Manually Opening UFDR report with the UFED Reader Program

In some cases, it may be necessary to manually open a UFDR report file with the UFED Reader program. After launching the UFED Reader program application, select *File > Open* from the upper left toolbar:



Then navigate to the location of the UFDR Report file to be opened:

| iPhone4GSM_7.0-7.0.2_Physical_13-11-13_08-50-47_2020-08-14_Report.ufdr | UFDR File |
|--|------------------------|
| 🔁 Cellebrite_Reader_v7.35_Jun_2020_Eng | Adobe Acrobat Document |
| 🔟 CellebriteReader | Application |
| Passwords | File folder |
| 📙 thumbnails | File folder |
| 📙 icons | File folder |
| 📕 gps | File folder |
| 📕 pages | File folder |
| party_photos | File folder |
| resources | File folder |
| 📙 Maps | File folder |
| 📙 files | File folder |
| 📕 email | File folder |
| L chats | File folder |

Time Zone Settings

Most mobile devices store the last time zone setting used. If present, Cellebrite will detect this information and indicate the time zone used upon opening the report:

| Device time zone detected | | × |
|---|----------------------------|------------------|
| The device's time zone was detected: (UTC-08:00) Los Would you like to adjust timestamps to the device's timestamps to the device | _Angeles (Amer me zone? | ica) . |
| Automatically adjust the time zone when device tim | ne zone informat | ion is available |
| | Yes | No |

9

It is usually beneficial to set the device to the time zone used to see the data time stamps in the user's local time. One exception could be when multiple devices from different time zones are being examined. By leaving the time settings in UTC, the common items will all display as the same time.

If the time zone was not adjusted to the detected time zone by the examiner or not detected automatically at the time of extraction, the time zone can be set manually from the Project Settings in the upper right of the Extraction Summary tab.

<u>Data Tabs</u>

Data tabs show files of a specific type such as call log, contacts, SMS messages etc. Data in data tabs display as a sub tab along the top, depending on the type of data:

- Text view View text files as text.
- Table view a list of all the files of a specific type.
- Thumbnail view view images by thumbnail.
- Folder view view the folder structure of the data files paths.
- Image view view the image.
- File Info view information about the file.

In the following example two sub tabs for Call Log and Device Locations are displayed. The numbers next to the name indicate how many records exist.

| | File View Tools Report Help | | | | | Advanced [10] 🐥 |
|------------------|---------------------------------------|--------------------------------|-----------------------------|---------------------------------|--|---|
| යි Home | ≪ ○ iPhone4GSM_7.0-7.0.2_Phys * : | Welcome × 🥥 Call | Log (13) O Device Locat | ions (281) | | ~) (~ |
| 0 | Search Q - | , | uly, 2013 | August, 2013 | September, 2 × Call Log | Go to 🔹 |
| Timalina | | | ٨ | | - + Timestamp: | 9/8/2013 6:19:47 PM(UTC+0) |
| | Analyzed Data | | | | Duration: | 00:02:04 |
| \sim | Application (59) | $\sqrt{\Lambda}$ | | | Status: | Answered |
| Analyzed Data | × 5 calls (12) | · · · | YE IE O Event - Eilter | e · Actions · Course | Country code | е |
| 1.0 | > \$ Call Log (13) | | vi⊧ si⊨ ∾ei Export • Fiitei | s · Acuons · Jasinon | Network Nan | e: |
| Cő | > A Contacts (22) | | * ® X K D G F | arties | ↓ Timestamp Source: | |
| - systems | | | 1 | From: 9732206574 Willie Steelum | 9/8/2013 6:19:47 Account: Video call: | |
| ÷Ó: | • •iv Devices & Networks (93) (31) | | 2 | From: 9732206574 Willie Steelum | 9/8/2013 6:19:07 Extraction: | Physical |
| Insights | ✓ V Location Related (282) (33) | s 🖬 | 3 | From: 6153567559 | 9/3/2013 1:02:45 | Data (Apple : HFS [+])/Data/wireless/Library/ CallHistory/call_history.db : 0x3E26 (Table: call, |
| R | > V Device Locations (281) (83) | | 4 | From: 6152288360 | 7/25/2013 8:09:4 | Size: 28672 bytes) |
| Tags | maps (i) | | 5 | From: 6152428276 | 7/23/2013 2:33:3 Parties | |
| _ | • • • • • • • • • • • • • • • • • • • | | 6 | From: 9732206574 Willie Steelum | 7/17/2013 1:26:1 | 732206574 Willie Steelum |
| E | Messages (180) (45) | | 7 | To: 6154956320 Jimmy Del ocke | 7/16/2013 2:17:1 | |
| Reports | > 9. Search & Web (148) (17) | | 8 | From: 0732206574 Willia Steelum | 7/16/2013 2:16:2 | |
| \bigcirc | > စြ) System & Logs (31) | | 0 | Ter 0703005574 Wille Greeker | 7/16/2013 1/26/0 | |
| Cloud | > 🏦 User Accounts & Details (43) (1) | | 9 | 10: 9732206574 Willie Steelum | 7/16/2013 1:26:0 | |
| | Data files | | 10 | To: 6154956320 Jimmy DeLocke | //1/2013 1:03:54 | |
| | | | 11 | From: 9732206574 Willie Steelum | 6/18/2013 5:48:0 | |
| | Applications (704) (2) | | 12 | From: 9732206574 Willie Steelum | 6/12/2013 9:03:0 | |
| | Archives (12) (4) | Total: 13 Deduplication: 0 Ite | ems: 13/13 Selected: 13 | | 2 | |
| | | | | | | |

UFDR REPORT – SEARCH, FILTER, TAG AND BOOKMARK

Searching Entire Extraction

To conduct a global search, enter the search term in the search box in the header shown below. This will show all a listing of the results in the data tabs where the search term was located.

| (i) | File View Tools Report Help | | | | | Advanced | ٠ |
|------------------|---|-------------------------|---|---|--|---|-----------|
| Ω Home | ≪ ○ iPhone4GSM_7.0-7.0.2_Phys * ا | Welcome × | Call Log (13) × (| O Device Locations (281) | iPhone465M Call Log Call Log | 7.0-7.0.2_Physical_13-11-16_0 (17) | w 3 |
| 0 | Search Q 👻 🗄 | | July, 2013 | August, 2013 | - + | Date: 9/8/2013 6:19:47 PM(UTC 10) (00:02 G Unknown: 9732206574 Willie Steelum Date: 9/8/2013 6:19:07 PM(UTC+0) (00:00 | io to 🔹 |
| ~~ | Analyzed Data | Λ | Λ | Λ_{M} | $ \land \land$ | Unknown: 9732206574 Willie Steelum Date: 7/17/2013 1:26:14 PM(UTC+0)(00:1). | |
| Analyzed Data | ✓ Calls (13) | S | • # # # Q | Export • Filters • Actions • Search | Q 3 | Chat: 19732206574 Meet me downstairs. New plan. (8/6/2013 Chat: + 19732206574 | |
| File Systems | Contacts (22) (4) Devices 6 Naturatio (02) (23) | | - 🖌 # 😒) 2 1 | | ↓ Timestamp 9/8/2013 6:19 17 ^ | (8/6/2013 12:40:15 PM(UTC+0)) Chat: Add me on Snapchatl Username: ovencas | |
| -Ò- Insights | • • • • • • • • • • • • • • • • • | | 2 3 | From: 9732206574 Willie Steelum From: 6153567559 From: 6153667559 | 9/8/2013 6:19 07 Contacts 9/3/2013 1:02:15 | Steelum Willie (1 entry, 0 addresses, +19732206574 ary) Willie Steelum (1 entry, 0 addresses, | / all, |
| No. Tags | | | 2 4 2 5 | From: 6152288360 | 7/25/2013 8:094 7/23/2013 2:33: | Usemame: (973) 220-6574 Willie Steelum (3 entries, 0 addresse User ID: 88BA2DA2-C80C-4258-AD5A-557 | |
| E | Messages (180) (45) | | 6 6 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 | From: 9732206574 Willie Steelum To: 6154956320 Jimmy DeLocke | 7/17/2013 1:26:1 SMS Messages 7/16/2013 2:17:1 2 | | |
| | Search & Web (148) (17) System & Logs (31) | | 8 | From: 9732206574 Willie Steelum To: 9732206574 Willie Steelum | 7/16/2013 2:16:2 7/16/2013 1:26:0 User Dictionary | To: +16154956320, +19732206577 Sent: 8/6/2013 12:32:34 PM(UTC+0): filder williesteelum | |
| Cloud | User Accounts & Details (43) (1) Data files | | 2 10 | To: 6154956320 Jimmy DeLocke | 2 7/1/2013 1:03:54 | williesteelum | |
| | Applications (704) (2) | | 12 | From: 9732206574 Willie Steelum | 6/12/2013 9:03:0 | | |
| | Archives (12) (4) | Total: 13 Deduplication | n: 0 Items: 13/13 Selec | cted: 13 | · · · · | | |

Searching individual data tab

Enter the search term in the search window shown below. The data table updates to display the results of the search.

| | File View Tools Report Help | | | Willie X • Advanced |
|--------------|---|--|---|--|
| යි Home | • iPhone4GSM_7.0-7.0.2_Phys • : | Welcome × Call Log (13) × | O Device Locations (281) × | * X |
| 0 | Search Q - | Juny, 2013 | August, 213 Septer | ber, 2 a Scall Log Go to • |
| Timeline | Analyzed Data | | | Timestamp: 9/8/2013 6:19:47 PM(UTC+0) Duration: 00:02:04 |
| | > Application (59) | $\langle \land \land \land \land$ | | Status: Answered |
| Data | 🐣 📞 Calls (13) | Clear filters 🛛 🐨 📰 🖓 | Export Filters • Actions Willie * | Country code: Network code: |
| to | > 🧐 Call Log (13) | 10 lm + 🦁 | 🗙 🔨 🗞 Parties 🔹 🖡 Timestamp | Source: |
| File Systems | Contacts (22) | I 🛛 1 | From: 9732206574 Willie Steelum 9/8/2013 6:19 | Account: Video call: |
| ÷ġ: | > () Devices & Networks (93) (31) | 2 | From: 9732206574 Willie Steelum 9/8/2013 6:19 | 107 PN Extraction: Physical |
| Insights | Cocation Related (282) (33) Device Locations (281) (221) | I 3 | From: 9732206574 Willie Steelum 7/17/2013 1:2 | 16:14 P Source file: Data (Apple : HFS [+])/Data/wireless/Library/ CallHistory/call_history.db : 0x3E26 (Table: call, |
| 0 | Device Locations (201) (33) Maps (1) | I 🗹 4 | From: 9732206574 Willie Steelum 7/16/2013 2:1 | 6:23 P Size: 28672 bytes) |
| Tags | > • Media (15388) (32) | 🖬 🖬 S | To: 9732206574 Willie Steelum 7/16/2013 1:2 | 16:04 P Parties |
| | > 📮 Messages (180) (45) | 6 | From: 9732206574 Willie Steelum 6/18/2013 5:4 | B:01 P |
| Reports | > Q Search & Web (148) (17) | 7 | From: 9732206574 Willie Steelum 6/12/2013 9:0 | 13:08 P |
| ~ | > 🗿 System & Logs (31) | | | |
| Cloud | > 🚨 User Accounts & Details (43) (1) | | | |
| | Data files | | | |
| | Applications (704) (2) | | | |
| | Archives (12) (4) | Total: 7 Deduplication: 0 Items: 7/13 Select | » ed: 7 | |
| | | | | |

Timeline Search

Timeline view is a powerful tool that enables you to analyze data in chronological order.

| | | | | • | `` | veid | come | · ^ | | × O Device Locations (281) × | Timeline (585) × | | | |
|--------------|---------|--------------|-----|---|----------|------|-----------------|------|------------------|--------------------------------------|--|--|----------------------|------------|
| | May, 20 | 13 | | | | _ | June | 2013 | | July, 2013 | August, 2013 | September, 2013 | October, 20 | 13 |
| | Apply | | | | | | | | | 1/1/2013 - 1/31/2013 | | | | $-\Xi$ |
| - | | | | | | | | | | | | | | Λ |
| | | | | | | ~ | | | | | | ~~~~~ | ~~~~ | Λ |
| | | | | | | | | | | | | | < | _ |
| | | | | | | | | | | Time | line settings 🥎 🕈 📴 🗧 | F BF Export ▼ Filters ▼ Actions | • Search | Q |
| | Doo | - ~ | # | 1 | \times | K | C | 0 | 📎 Туре 🔹 | † Timestamp | Party • | Description | Source • | 오 Sou |
| | ۰. | \checkmark | 190 | | | | | | Images | 7/30/2013 12:14:59 PM [Capture Time] | | IMG_0011JPG | | IM |
| | ۰. | V | 191 | | | | | | Instant Messages | 7/30/2013 10:06:31 PM(UTC+0) | | Add me on Snapchat! Username: jdelock | SMS Spotlight Search | sms SM |
| | ۰. | V | 192 | | | | ۰۴ | | SMS Messages | 7/30/2013 10:06:31 PM(UTC+0) | From: +16154956320 Ji To: +16155079714 | Add me on Snapchat! Username: jdelock | | sm: |
| | ۰. | | 193 | | | | | | Instant Messages | 7/30/2013 10:09:35 PM(UTC+0) | | Hit me on my burner at +18327865698 if | SMS Spotlight Search | sms SM |
| | | | 194 | | | | لا | | SMS Messages | 7/30/2013 10:09:35 PM(UTC+0) | From: +16154956320 Ji To: +16155079714 | Hit me on my burner at +18327865698 if | | sms sms |
| ^ 7/3 | | | | | | | | | | | | | | |
| | • | V | 195 | | | | ر لا | | Emails | 7/31/2013 12:03:19 AM(UTC+0) | From: itunes@new.itune To: owenucash2@gmail | <idoctype "-="" dtd<="" html="" public="" td="" w3c=""><td>Mails</td><td>Env Pro</td></idoctype> | Mails | Env Pro |
| | | | 105 | | | | e۲ | | Emaile | 7/31/2013 12:22:47 PM(LITC+0) | From: News@InsideAppl | <idoctype "-="" dtd<="" html="" public="" td="" w3c=""><td>Mails</td><td>Em</td></idoctype> | Mails | Em |

Filtering and Sorting

In any Analyzed data or Data file window, the listed results are filtered by column. Click on the relevant column heading to view filter and sort options.

| | | | J.2 | • | N | (elc | ome | × | Call Log (13) | × | O De | evice | Locat | tions | (281) | × | • 1 | imeline | : (585 |) × | | | | | | | | |
|--------------------|---------|--------------|-----|---|---|------|---------|-----|-------------------|----------|---------|--------|--------|-----------|--------|------|----------|---------|--------|------|---------|--------|-------|--------|--------------------|----------------------|---------|-----|
| _ | May, 20 | 013 | | | | | June, 2 | 013 | | | July, 2 | 013 | 7/1/20 | 013 - 7/3 | 31/201 | 3 | | August, | 2013 | | | | | Se | ptember, 2013 | Octobe | r, 2013 | - |
| | Apply | | | | | | | | | | | | | | | | | | | | | | | | | | | Ξ |
| - | | - | | | | | | | | | | | | | | | _ | | | | | | | | | | | |
| | | | | | | | | | | \wedge | | | | Λ | | | Λ | | | | | | | _ | | \wedge | - 1 | Ł |
| | | | | | | | | | | | | | | | | | | | | | | | | | | < | - | 1 |
| | | | | | | | | | | | | | | | | Time | line set | tings | 5∙ | Your | | E 1 | xport | ▼ Filt | ers Actions | Search | | ۹ |
| 60 | Doo | - ~ | # | 1 | × | Κ | SI | 20 | 🤊 Туре 🗸 | 1 Tim | iestam | p | | | | • | Part | y | | • | Des | script | ion | | | Source | • 2 | So |
| | | | 190 | | | | | (| Images | \$1 s | ort Aso | ending | | | | | al. | | | | | | | | | | | IN |
| | - | - | 101 | | | | | ` | / Instant Manager | Z S | ort Des | cendir | ng | | | | | | | | | | | | and interference | CMC Constitute Count | | |
| | • | <u>v</u> | 191 | | | | | | Instant Messages | ×7 c | | | | | | | | | | | | | | | ime: Jdelock | SMS Spotlight Search | | Sh |
| | | \checkmark | 192 | | | | رلا | | SMS Messages | F | rom: | | | | | | | To: | | | | | | | ime: jdelock | | | sm |
| | - | | | | | | | | | _ | | | Aug | just, 20 | 020 | | > | < | | Au | gust, 2 | 2020 | | > | | | | sm |
| | ۰. | \checkmark | 193 | | | | | | Instant Messages | | Su | Mo | Tu | We | Th | Fr | Sa. | Su | Мо | Tu | We | Th | Fr | Sa | \$27865698 if | SMS Spotlight Search | | SIT |
| | - | | 194 | | | | eK | | SMS Messages | | 26 | 27 | 28 | 29 | 30 | 31 | 1 | 26 | 27 | 28 | 29 | 30 | 31 | 1 | 27865698 if | | | sm |
| | | - | | | | | Ĩ | | Sins measures | | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | n. 1 0 0 0 0 0 0 1 | | | sm |
| | | | | | | | | | | | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | | | | |
| | | | 195 | | | | بد | | Emails | | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | //W3C//DTD | Mails | | En |
| ^ 7/3 | | _ | | | | | - | | | | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | | | | Pre |
| ^ 7/3 | • | | | | | | | | | | 30 | 31 | 1 | 2 | 3 | 4 | 5 | 30 | 31 | 1 | 2 | 3 | 4 | 5 | | | | |
| ∧ 7/3 [∞] | • | _ | | | | | -K | | | | | | | | | | | | | | | | | | | | | |

Conversation view

Communication-based data (text messages) can be displayed in a conversation view layout between two or more parties that resemble what the user would see on their device.

Open Conversation View

Use the conversation view button to see all related messages in a threaded view:

| | SMS | Messag | ges (3 | 5) | | | | | | | | | | | |
|--------|-----|-----------------------|----------|-----|----------|------|------------|--|-----------|------------------|--|---|--|--|---------------|
| ¥== ¥= | | 3 • Q | n ©⊕ (| 9 🕸 | | Expo | ort • | V. | | Table Search 🗸 🔍 | | | SMS Messa | Go to | |
| | 000 | - ~ | # | 1 | \times | ĸ | Ç | ↓ Timestamp | Delivered | • | Read | | Source: | | |
| | | ✓ | 13 14 | | × | | থ থ | 8/6/2013 5:35:07 AM(UTC-7) 8/6/2013 5:32:34 AM(UTC-7) | | | | | Folder: | Sent 8/6/2013 5:32:34 | AM(UTC-7 |
| | | √ | 15 | | | | د™ •⊀ | 8/6/2013 5:32:18 AM(UTC-7) | | | 0/6/2012 5 22 47 444 | | Delivered: Read: Status: S | Sent | |
| | | | 10 | | | | ريد ريد | 8/6/2013 2:26:59 AM(UTC-7) 8/4/2013 7:39:20 AM(UTC-7) | | | 8/6/2013 5:23:47 AM 8/5/2013 6:27:04 AM | U | Extraction: | Physical | |
| | | | 18 | | | | رلا | 8/3/2013 7:20:43 AM(UTC-7) | | | 8/5/2013 6:27:04 AM | U | All timestamps | | |
| | | | 19 | | | | ولا | 8/1/2013 2:32:54 PM(UTC-7) | | | 8/5/2013 6:27:11 AM | U | Parties | | |
| | | | 20 | | | | رد دلا | 7/30/2013 3:09:35 PM(UTC-7) | | | 8/5/2013 6:27:13 AM | U | To: +1615495 To: +1973220 | 56320 Jimmy De 06574 Willie Ste | Locke elum |
| | | | 21 | | | | e v | 7/30/2013 3:06:31 PM(UTC-7) | | | 8/5/2013 6:27:13 AM | U | Body 💌 | 14 | |
| | | | 22 | | | | ولا | 7/5/2013 3:03:59 PM(UTC-7) 7/5/2013 3:03:58 PM(UTC-7) | | | 7/5/2013 4:55:18 PM(| u | Add me on Si owencash htt download?rei | napchat! Usernan :p://snapchat.com f=a | ne: / |

Conversation View Example



Using the Quick Filter

To improve accessibility the filters are now grouped under simple menus.



<u>Tags</u>

The investigator can tag items for future reference and quickly generate a report from tagged items. Each item can have multiple tags. To add a tag to timeline items:

- 1. Select one or more row in the timeline table.
- 2. Click 🔊 .
- 3. Select Tag.
- 4. Select the required tags.

| Search tags Q → Clear All Case tags | <u>Manag</u> | <u>e tags</u> |
|---|--------------|---------------|
| Evidence (F6) Important (F7) Pending (F8) Completed (F9) | | |
| | | |
| Description (optional) | | |
| | OK Car | ncel |

5. Click OK.

Manage Tags

- 1. Click 🔊 .
- 2. Select Manage tags.
- 3. In the Manage tags window you can:
 - Search tags.
 - Rename existing tags.
 - Delete tags.
 - Define tag color.
 - Define tag hotkey.
 - Create a new tag by clicking <u>New tag</u>.

| 🚇 Manage tags | | × |
|---|------------|---------|
| Define your tags names, colors and hotkeys. | | |
| Search tags Q = | | |
| Case tans | | |
| Case tags | | New tag |
| 🗑 Evidence | ▼ F6 | Ŧ |
| 🍟 Important | F 7 | • |
| Pending | F 8 | Ŧ |
| Completed | F 9 | Ŧ |
| Project VIC categories | | |
| | | |
| | ок | Cancel |

4. Click Ok.

Bookmarking

Using the UFED Reader application, any relevant data identified can be bookmarked for inclusion in the report. To include items in a report, the check box next to the data item(s) must be selected as follows:

| (i) | File View Tools Report Help | | | Willie | × · · Advanced |
|-----------------------|---|--|---|--|--|
| ⇔ Home | • iPhone4GSM_7.0-7.0.2_Phys • : | Welcome × O Call Lo | ng (13) × O Device Locations (281) × | Timeline (585) × O Chat (Chats) (25) × | SMS Spotlight Search Chat (2) × |
| () Timeline | Search Q I * E | Apply | 7/1/2 | 013 - 7/31/2013 | Ç |
| - Analyzed Data | Analyzed Data Application (59) | | | | Messages |
| File Systems | Calls (13) Call Log (13) Contacts (22) | | S × ∧ | Se E Export Hiters Action Timestamp Party | Description |
| ·Ò- Insights | (1) Devices & Networks (93) (31) Q Location Related (282) (33) | | 190 ♥ images 191 I I I Instant Messages | 7/30/2013 12:14:59 PM [Capture Time] 7/30/2013 10:06:31 PM(UTC+0) | Add me on Snapchatl Username: |
| T ags | O Device Locations (281) (33) O Maps (1) Media (15388) (32) | | 192 SMS Messages 193 Instant Messages | 7/30/2013 10:06:31 PM(UTC+0) From: +161: To: +16150 7/30/2013 10:09:35 PM(UTC+0) | 54956320 Ji Add me on Snapchatl Username: 79714 Hit me on my burner at +183278 |
| Reports | Messages (180) (45) Chats (25) (3) | . 2 | 194 🥊 SMS Messages | 7/30/2013 10:09:35 PM(UTC+0) From: +161 To: +161550 | 54956320 Ji Hit me on my burner at +183278 179714 |
| Cloud | Emails (119) (39) | 7/31/2013 (3) ■ | 195 🥊 Emails | 7/31/2013 12:03:19 AM(UTC+0) From: itune: To: owenuca | @new.itune <idoctype *-="" html="" public="" w:<br="">sh2@gmail</idoctype> |
| | > Q. Search & Web (148) (17) > 중) System & Logs (31) | | 196 🥲 Emails | 7/31/2013 12:22:47 PM(UTC+0) From: News To: owenuca | @InsideAppl HTML PUBLIC *-//W:<br sh2@gmail |
| | > 🏦 User Accounts & Details (43) (1) | Total: 585 Deduplication: 0 Ite | ms: 585/585 Selected: 585 | | > |

CREATING CUSTOM REPORTS

(See the Cellebrite UFED Reader manual for further information on creating reports)

Using the UFED Reader application, any relevant data identified can be bookmarked for inclusion in the report. A new report is created from the Extraction Summary tab:

| Welcome × 🥚 | Extraction Summary (1) × O SMS Messages (35) | × o d | Conversation (SMS Mes | ssage) \times | | | - |
|---|--|--------|---------------------------------------|-----------------|--------------------|------------|------------|
| All Content | Physical | | | | | | |
| Extraction Su | mmary | | + Add extraction (2) Project settings | | | 🗎 Generate | report |
| ⊙ Extractions: 1 | | | | | | | |
| - | Physical 🖉 | | | | | | |
| | Physical | | | | | | |
| and the second se | Extraction start date/time | | | | | | |
| | Extraction end date/time | | | | | | |
| _ | F:\Sample Reports 03022018\2018-03-02 | | | | | | |
| Case Information | | | | | | | |
| Case number | Apple iPhone 4 Test Case | | Case name | Sample | | | |
| Evidence number | I-0001 | | Examiner name | JNO | | | |
| Department | IRIS LLC | | Location | PO Box 340355, | Hartford, CT 06134 | | |
| | 120 1 | ^ | Device Content | | | | \bigcirc |
| Apple ID Apple ID | owenucash2@gmail.com | | | | | | |
| Apple ID | owenucash2@gmail.com | _ | Phone Data | | | | |
| Apple ID | owenucash2@gmail.com | | Application Usa | age 8 | 📞 Call Log | 13 | |
| Apple ID Apple ID | owenucash2@gmail.com owenucash2@gmail.com | | and the | | | | |
| OS Version | iPhone OS 7.0.2 (11A501) | | Coll Towers | 45 | O. Chate | 25 (2) | |
| Last Factory Restore Up Phone date/time | grade 9/27/2013 2:06:04 PM(UTC 10/17/2013 8:12:08 PM/UT | | | | -er chuts | 25 (5) | |
| Last user ICCID | 89014102276076832607 | | | | @ | 70.007 | |
| ICCID | 89014102276076832607 | \sim | (8) Contacts | 9 | Cookies | /9 (1/) | \sim |

Select the desired report format(s) and input any case information:

| General | General | |
|-----------------------|-----------------------|--|
| Report Dataset | | Drone, DJI- Jnspire 2, 2017-12-25, Report |
| Drone_DJI - Inspire 2 | Save to: | \\ptnas1\Home_Dirs\jonathank\Documents\My Reports Browse |
| _IPhoNe 4-18models | Report sub directory: | 2017-12-25.11-23-12 |
| Cocurity | Project | Drone_DJI - Inspire 2; _JPhoNe 4-18models |
| security | Format | |
| Layout | Case Information | UFDR (For Reader or Analytics Desktop) |
| Default sorting | Case number: | PDF Report |
| | Case name: | |
| | Evidence number: | |
| | Examiner name: | Excel Workbook (xlsx) |
| | Department: | Excel 97-2003 (xls) |
| | Location: | Word report |
| | Notes: | XML Report |
| | | Close |
| | | L |
| | | |

Specific data types can be selected for inclusion in the report:

| General | Report Dataset - Multi-project | |
|-----------------|---|--|
| Report Dataset | Select/Deselect All | |
| | Extraction | |
| Multi-project | | Enter text to filter |
| Security | Application Usage (864/864) Applications (2230/2230) | ✓ Locations (285/285) ✓ Notifications (26/26) |
| Layout | Audio (157/157) Calendar (24/24) | Passwords (28/28) Report Evidence - Notes (1/1) |
| Default sorting | Call Log (6/6) Call Call Cold (6/6) Camera Evidence - Uncategorized (4/4) | Powering Events (45/45) Searched Items (17/17) |
| PDF Report | Chats (75/75) Configurations (86/86) Contacts (283/283) Cookies (462/462) Databases (417/417) Device Info (34/34) Device Users (1/1) Documents (5/5) Emails (235/235) Images (1810/1810) Installed Applications (220/220) | ✓ SMS Messages (27/27) ✓ Text (1372/1372) ✓ Timeline (1729/1729) ■ Uncategorized (11818/11818) ✓ User Accounts (19/19) ✓ User Dictionary (176/176) ✓ Videos (78/78) ✓ Web Bookmarks (4/4) ✓ Web History (42/42) ✓ Wireless Networks (280/280) |
| | | |
| | Tags (0/0) Calculate SHA-2 (256 bit) hash Calculate MD5 (128 bit) hash Include translations Include system images | Tags only (0/0) Redact image thumbnails Include merged items (analyzed data) Include merged items (data files) Include source info indication Include enrichments Hide extraction source indication Include account package |
| | Analytics | |
| | Activity Analytics (370/370) Analytics Emails (39/39) Analytics Phones (149/149) | |
| | Previou | s Next Finish Cance |

Export Single Report Items

Use the export drop down box and select the desired output format for individual item reports:

| Export - 🕫 🗞 🔯 Enter text to filter 🗙 |
|---|
| Participants (3) |
| Jimmy DeLocke +16154956320 Willie Steelum +19732206574 +16155079714 |
| Conversation |
| - ✓ Select/Deselect all 4 messages |
| From: Jimmy DeLocke |
| Add me on Snapchat! Username: jdelocke http://snapchat.com/download?ref=a |
| 7/30/2013 3:06:31 PM(UTC-7) |
| |
| From: Jimmy DeLocke |
| Hit me on my burner at +18327865698 if you want to connect! Get your own at http://brnr.me/c4dK |
| //30/2013 3:09:35 PM(UTC-7) |
| To: Unknown |
| Add me on Snapchat! Username: owencash http://snapchat.com/download?ref=a |
| 8/6/2013 5:32:34 AM(UTC-7) |
| |
| To: Wille Steelum |
| Meet me downstairs. New plan. |
| 67672015 54037 AWIOTC77 |
| |
| 17 |

REQUESTING REPORTS

When dealing with digital evidence from a mobile device that has been preserved and examined by law enforcement, industry standards recommend that a full report and copy of the original extraction file and proprietary file viewer be requested.

When requesting Cellebrite reports, the entire extraction should be requested in PDF, HTML and UFDR style formats. The UFED Reader program and manual should be requested as well as the copy of the forensic extraction in the native proprietary format.

Sample Request

- 1. All reports including search warrant or consent, and reports regarding the seizure and the chain of custody of the evidence.
- 2. The forensic examiners report detailing the tools and all procedures used to examine the device.
- 3. A copy of the extraction file in the native (original) format of the forensic device or software used to conduct the extraction.
- 4. Full forensic extraction report in PDF and HTML format.
- 5. Forensic Report in UFED Reader format with UFED Reader file viewer.
- 6. The proprietary file viewer for the specific forensic tool used to create the extraction.

SUMMARY

A logical extraction is fast and easy, but will not recover deleted data.

A physical extraction will get the most data, but could take much longer to run.

Not all devices are supported for all levels of extraction.

The report could be in three (3) different format types.

Save extraction reports to desktop for faster file access.

Be sure you are aware of the time setting that was set for the report.

The PDF Report needs to be opened using Adobe Reader for the link files to work.

HTML link files will open in your internet browser and may bring you to the website visited.

When viewing HTML reports, keyword searches are available only if the tab of the desired area has been opened.

The Cellebrite UFED Reader Program is needed to open UFDR Report.

The links will not work if both the report and associated link file folders are not provided or are not together.

Be sure to request the forensic extraction in its native proprietary format.

HINTS

<u>UTC Time</u> **EST** = Eastern Standard Time (UTC - 5 hours), (Autumn/Winter) **EDT** = Eastern Daylight Time (UTC - 4 hours) (Spring/Summer)

<u>Rapid assessment</u> Navigate to the timeline to review activities around the time of incident.

<u>Locating email addresses</u> Use @ symbol in keyword searches to find email addresses.

<u>Creating Custom Reports</u> See the UFED manual for further information on generating reports using the UFED Reader.

For More Information Visit our website at <u>www.elabforensics.com</u> or call us directly **877-266-3703**.

References www.cellebrite.com